

WHAT IS CLAIMED IS:

1. A method for auditing the security of an enterprise including plural nodes comprising:

collecting security information from the nodes of the enterprise under audit;
analyzing the security information and providing a first result of this analysis; and
comparing this first result with a second result comprising security standards applicable to the enterprise under audit and one or more other enterprises that together form a relevant peer group, the result of this comparing step indicating the relative security of the enterprise under audit relative to that of the peer group of enterprises.

2. The method of claim 1 wherein, in the comparing step, the second result comprises information derived from industry standards applicable to the relevant peer group of enterprises.

3. The method of claim 1 wherein, in the comparing step, the second result comprises information derived from information previously obtained through application of the collecting and analyzing steps to two or more enterprises in the relevant peer group.

4. The method of claim 1, further comprising the step of generating at least one report that presents the first and second results arranged in a way that facilitates their comparison.

5. The method of claim 4 wherein the generating step includes presenting the first and second results each broken down into several results relating to several different areas of security, with a first and a second result presented for each different area of security and arranged in a way that facilitates their comparison.

6. The method of claim 5 wherein, in the generating step, the results relating to several different areas of security comprise results arising from analysis of personnel security information and physical security information, at least some of the information included in the first result having been gathered using interviews during the collecting step.

7. The method of claim 5 wherein, in the generating step, the results relating to several different areas of security comprise results arising from analysis of password security information and file access permission security information.

8. The method of claim 7 wherein, in the generating step, the results relating to several different areas of security further comprise results arising from analysis of personnel security information and physical security information, at least some of the information included in the first result having been gathered using interviews during the collecting step.

9. The method of claim 5 wherein, in the generating step, the several

different areas of security comprise one or more results of analysis of node configuration security information and one or more results of analysis of security information gathered using interviews.

10. The method of claim 9 wherein, in the generating step, the one or more results of analysis of node configuration security information comprise results arising from analysis of password security information.

11. The method of claim 9 wherein, in the generating step, the one or more results of analysis of node configuration security information comprises results arising from analysis of file access permission security information.

12. The method of claim 4, wherein the generating step generates at least two comparative reports in different formats for different requesting parties or uses, and in particular one for technical experts that includes technical language and details and another for non-technical-experts that substantially excludes technical language and details.

13. The method of claim 1, to which is added:
generating and executing commands to alter the security information of one or more nodes to improve system security in at least some cases when the analysis or comparison or both indicate security is in need of improvement.

14. The method of claim 13, further comprising;
generating at least one report that presents the first and second results arranged in a way that facilitates their comparison.

15. The method of claim 13 wherein the generating commands step generates commands which force the deactivation or correction of one or more passwords when the analysis or comparison or both indicate that these one or more passwords are not sufficiently secure.

16. The method of claim 13 wherein the generating commands step generates commands which force alteration of one or more configuration file or control file access permissions if the analysis or comparison or both indicate that the access permissions assigned to these one or more files do not provide adequate system security.

17. A system for auditing the security of an enterprise comprising:
a plurality of nodes within the enterprise under audit;
collectors associated with the nodes and arranged to collect from the nodes information concerning the security of the enterprise under audit;
a security analyzer arranged to analyze the information concerning the

security of the enterprise under audit and to provide a first result of this analysis;

a data base containing a second result comprising security standards applicable to the enterprise under audit and one or more other enterprises that together form a relevant peer group; and

a comparison mechanism arranged to compare the first and second results to determine the relative security of the enterprise under audit in comparison to that of the enterprises in the relevant peer group.

18. A system in accordance with claim 17 to which is added:

a report generator that generates at least one report which presents the first and second results arranged each broken down into several results relating to several different areas of security, with a first and second result presented for each different area of security and arranged in a way that facilitates their comparison.

19. A system in accordance with claim 17 to which is added:

change agents associated with the nodes and able to execute commands that alter node configuration information; and

a command generator that provides commands to the change agents on selected nodes to alter node configuration information to improve system security in response to the analyzer or comparison mechanism or both determining security improvements are needed.

20. A system in accordance with claim 19 wherein the command generator includes a mechanism that can generate commands which, when executed, cause one or more of the change agents to force the deactivation or correction of one or more secure passwords if the security analyzer or comparison mechanism or both determine that one or more passwords are not sufficiently secure.

21. A system in accordance with claim 19 wherein the command generator included a mechanism that can generate commands which, when executed, cause one or more of the change agents to force the alteration of the access permissions of one or more configuration files or control files if the security analyzer or comparison mechanism or both determine that the access permissions assigned to one or more such files do not provide sufficient security.

22. A system for auditing the security of an enterprise comprising:

a plurality of nodes within an enterprise under audit;

collector means associated with the nodes for collecting information from the nodes concerning the security of the enterprise under audit;

security analyzer means for analyzing the information concerning the

security of the enterprise under audit and for providing a first result of this analysis;

data base means for storing and for presenting a second result comprising security standards applicable to the enterprise under audit and one or more other enterprises that together form a relevant peer group; and

comparison means for comparing the first and second results to determine the relative security of the enterprise under audit in comparison to that of the enterprises in the relevant peer group.

23. A system in accordance with claim 22 to which is added

report generation means for generating at least one report which presents the first and second results each broken down into several results relating to several different areas of security, with a first and second result presented for each different area of security and arranged in a way that facilitates their comparison.

24. A system in accordance with claim 22 to which is added

change agent means associated with the nodes for executing commands that alter node configuration information; and

command generator means for providing commands to the change agent means on selected nodes as needed to alter system configuration information to improve system security in response to the security analyzer means or the comparison means or both determining that security improvements are needed.